REMARKS

The foregoing Amendment After Final and the following Remarks are submitted in response to the Final Office Action issued on May 20, 2005 in connection with the above-identified patent application, and are being filed within the three-month shortened statutory period set for a response by the Final Office Action. Applicants respectfully request entry of the Amendment in that the Amendment raises no new issues and requires no further searching, in that the Amendment is believed to place the application in condition for allowance, and in that no new matter has been added to the application by the Amendment.

Claims 1, 3-22, 25, 27-30, 33, and 35-37 are pending in the present application as amended. Claim 1 has been amended to include the subject matter of claim 2 and accordingly claims 3-7 have been amended to adjust dependencies. Claim 10 has been amended to include the subject matter of claims 23, 24, and 26 and accordingly claims 25 and 27 have been amended to adjust dependencies. Claim 30 has been amended to include the subject matter of claims 31, 32, and 34 and accordingly claims 33 and 35 have been amended to adjust dependencies. Claims 38-50 have been canceled.

The Examiner has rejected the pending claims under 35 USC § 103(a) as being obvious over Ginter (U.S. Patent No. 5,910,987). Applicants respectfully traverse the § 103(a) rejection insofar as it may be applied to the claims as amended.

Independent claim 1 as filed recited an apparatus for producing a new ((n)th) black box for a digital rights management (DRM) system, where the (n)th black box is for being installed in the DRM system and for performing decryption and encryption functions in the DRM system. The (n)th black box is produced and delivered to the DRM system upon request therefrom and includes a new ((n)th) executable and a new ((n)th) key file. The (n)th key file has a new ((n)th) set of black box keys and a number of old sets of black box keys, and the request includes an old ((n-1)th) key file having the old sets of black box keys.

In the apparatus, a code optimizer / randomizer receives a master executable and randomized optimization parameters as inputs and produces the (n)th executable as an output. Also, a key manager receives the (n-1)th key file and the (n)th set of black box keys as input, extracts the old sets of black box keys from the (n-1)th key file, and produces the (n)th key file including the (n)th set of black box keys and the old sets of black box keys as an output. The (n)th executable and the (n)th key file are to be forwarded to the requesting DRM system.

As amended, claim 1 further recites that the key manager produces the (n)th key file encrypted according to a secret, and that the apparatus further comprises an injector receiving the (n)th executable from the code optimizer / randomizer as an input, injecting the secret into the (n)th executable in a pre-determined location, and producing the injected (n)th executable as an output. The injected (n)th executable and the encrypted (n)th key file are to be forwarded to the requesting DRM system.

Independent claim 10 substantially recites the subject matter of claim 1, although in the form of a method. Independent claim 30 recites a method such as that of claim 10 but focuses on producing the executable only.

As was previously pointed out, and as set forth in the specification of the present application, a license server only issues a license to a DRM system that is 'trusted' (i.e., that can authenticate itself). To implement 'trust', the DRM system is equipped with a 'black box' that performs decryption and encryption functions for such DRM system. The black box includes a public / private key pair, a version number and a unique signature, all as provided by an approved certifying authority. The public key is made available to the license server for purposes of encrypting portions of the issued license, thereby binding such license to such black box. The private key is available to the black box only, and not to the user or anyone else, for purposes of decrypting information encrypted with the corresponding public key.

From time to time, the DRM system may obtain a new and unique ('individualized') black box from a black box server or the like, and such black box server delivers the individualized black box with a new public / private key pair (PU-BB, PR-BB). The black box server may choose to individualize each black box by individualizing an executable program file that is delivered to and is resident on the DRM system. Such executable program file may for example be a dynamically linked library file or the like.

The black box server delivers the new individualized black box executable with a new public / private key pair (PU-BB, PR-BB). However, the new individualized black box executable should still be able to employ old key sets previously delivered to the DRM system in connection with old executables. As may be appreciated, such old key sets are still necessary to access older digital content 12 and older corresponding licenses 16 that were generated according to such old key sets. Accordingly, with the present invention as recited in claims 1-50, such new individualized executable is provided with access to old key sets and old public / private key pairs.

The Ginter reference discloses a system and method for secure transaction management and electronic rights protection, where electronic appliances such as computers participate in the system to ensure that information is accessed and used only in an authorized manner. Thus, such electronic appliances provide a distributed virtual distribution environment (VDE) that may enforce a secure chain of handling and control.

As set forth at column 12, such Ginter VDE can employ among other things a distributed, secure, "virtual black box" comprised of nodes located at every user site. The nodes of such virtual black box can include a secure subsystem having at least one secure hardware or software element. In addition, the Ginter VDE can include encryption and decryption means, secure communications means employing authentication, digital signing, and encrypted transmissions, where the secure subsystems at the user nodes utilize a protocol that establishes and authenticates each node's and/or participant's identity, and establishes one or more secure host-to-host encryption keys for communications between the secure subsystems.

However, and as was previously argued, the Ginter reference does not at all appreciate that the Ginter black box should be or could be periodically updated by obtaining from a centralized black box server a new individualized black box and a corresponding new set of black box keys, as is set forth in claims 1 et seq. Consequently, the Ginter reference does not at all appreciate that such new set of black box keys should or could be contained in a key file with previous sets of black box keys, as is set forth in claims 1 et seq. so that such previous sets of keys are available for use should the need arise.

Applicants again respectfully submit that the Ginter reference does not disclose that a node thereof can or should request a new black box, and thus does not disclose that such a request for an (n)th black box should or could be processed by a code optimizer / randomizer in the manner recited in claims 1 et seq. Likewise, the Ginter reference does not in fact disclose that a node thereof can or should request a key file in the manner recited in claims 1 et seq., and thus does not disclose that such a request for such a key file should or could be processed by a key manager in the manner recited in claims 1 et seq.

Moreover, Applicants also again respectfully submit that the Ginter reference does not contemplate updating the black box thereof by obtaining a new individualized black box and a corresponding new set of black box keys, where the new set of black box keys is contained in a key file with previous sets of black box keys. Thus, the Ginter system as disclosed does not forward any (n)th executable and (n)th key file to a requesting node in the manner set forth in claims 1 et seq.

Finally, Applicants respectfully submit that inasmuch as the Ginter reference does not at all disclose or even suggest that a centralized key manager should or could produce the (n)th key file encrypted according to a secret, as is required by claims 1 et seq., or that an injector should or could be employed to receive the (n)th executable from a code optimizer / randomizer as an input, inject such a secret into the (n)th executable in a pre-determined location, and produce the injected (n)th executable as an output, wherein the injected (n)th executable and the encrypted (n)th key file are to be forwarded to a requesting DRM system, all as required by claims 1 et seq.

Thus, because the Ginter reference does not disclose, suggest, or teach such injection of such a secret into an executable, in addition to the requirement for obtaining a new black box including a new executable and a new key file in the manner set forth in claims 1 et seq., Applicants respectfully submit that such Ginter reference cannot be applied to make obvious claims 1, 10, or 30, or any claims depending therefrom. Instead, Applicants respectfully submit that such claims are not in fact obvious in view of the Ginter reference, and accordingly, Applicants respectfully request reconsideration and withdrawal of the § 103(a) rejection.

In view of the foregoing discussion, Applicants respectfully submit that the present application including claims 1, 3-22, 25, 27-30, 33, and 35-37 is in condition for allowance, and such action is respectfully requested.

Respectfully Submitted,

Date: July 20, 2005

Steven H. Meyer
Registration No. 37,189

Woodcock Washburn LLP
One Liberty Place - 46th Floor
Philadelphia PA 19103
Telephone: (215) 568-3100
Facsimile: (215) 568-3439